GUIDE - 3250.26
GENERAL MANAGEMENT AND ADMINISTRATION

FOOD AND DRUG ADMINISTRATION

INFORMATION RESOURCES MANAGEMENT - INFORMATION TECHNOLOGY SECURITY

ADMINISTRATIVE SECURITY - CONTROL SELECTION

1. **PURPOSE.** The purpose of this document is to outline the overall Agency-wide policy for the selection of controls used to protect Food and Drug Administration (FDA) information systems. The policy describes the general requirements for the assignment and implementation of system security controls to meet the basic goals of protecting FDA automated information; assuring operational continuity, integrity, availability, and confidentiality of automated information; reducing Information Technology (IT) security risk; and, complying with applicable rules and regulations. The policy also outlines the responsibilities of key personnel in support of such requirements.

   BACKGROUND. The requirement exists through other policy documents to implement security controls on information systems. This necessitates the establishment of policies regarding the nature and extent of such controls. In accordance with Federal mandates (see 3. References), the FDA is required to provide "adequate security" to manage potential risk to its automated information. Adequate security includes the selection and employment of suitable security controls for use on Agency information systems. Proper control selection allows management to eliminate or mitigate the risk and magnitude of the harm which future incidents can cause and which could adversely affect the ability of FDA to

2. **REFERENCES.**

   Computer Security Act of 1987

   Computer Fraud and Abuse Act of 1986

   Clinger-Cohen Act of 1996

   Paperwork Reduction Act of 1995

   Federal Managers Financial Integrity Act

   Government Information Security Reform Act (GISRA)

   Office of Management and Budget (OMB) Circular A-130, Appendix III, "Management of Federal Information Resources," Revised 2/96

DHHS Automated Information Systems Security Program Handbook (Release 2.0), 5/94

Personnel Security/Suitability Program, DHHS Personnel Manual, 1/98

National Institute of Standards and Technology (NIST) Special Publications:

NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, 10/95

NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, 9/96

NIST Special Publication: Information Technology Security Training Requirements: A Role and Performance-Based Model, 1998

NIST User Guide for Developing and Evaluating Security Plans for Unclassified Federal Automated Information Systems (Draft version 6.03)

FDA security plan formats

FDA contingency plan formats

FDA model security (hypothetical) plans

3. **POLICY.** It is the policy of FDA to implement and maintain security controls on all its information systems. Each computer system will have a risk assessment-based independent security system review incorporated into its development life cycle. Risk assessments will be reviewed on a periodic basis. Each Center/Office must assure that its security control selection programs meet FDA security goals by compliance with the following requirements:
    a. **Controls And Systems Design.**
        1. Information must be protected in a manner commensurate with its sensitivity, value, and criticality. This policy applies regardless of the media on which information is stored, the locations where the information is stored, the systems used to process the information, or the processes by which information is handled.
        2. All computer and communications security measures must be simple and easy to use, administer, and audit.
        3. For all business application systems, security must be considered by systems designers and developers from the beginning of the systems design process through conversion to a mission critical system. Part of a commercial, off-the-shelf (COTS) evaluation must be an evaluation of the adequacy of the security controls provided by the COTS. If the COTS does not provide adequate

security, it is either not appropriate or must be encapsulated in an environment where the security is provided.

4. Within the confines of cost-justification, information security controls must be selected and designed such that reliance on a common mechanism is minimized. Systems must avoid any design which provides a single point of failure for all protections. The security of a computer system must never be entirely dependent on the security of another computer system.
5. When designing information security measures, users must use large margins of error and large time horizons. For example, encryption key lengths must be sufficiently large so that encryption systems will not be likely to be defeated within the next decade.
6. All systems interfacing external networks (Internet firewalls, Internet commerce servers, dial-up modem banks, etc.) must be running the latest version of the vendor-supplied operating software, to include all applicable updates, fixes, service packs, and patches. To take advantage of recent security improvements, FDA must use the most recent version of all multi-user computer operating systems. Information systems security products on the market less than a year must not be used as an integral component of any FDA mission critical information system.
7. To ensure that FDA technical staff has taken appropriate preventive measures, all systems connected to the Internet without protective technology (such as a firewall) must be subjected to an automated risk assessment performed via vulnerability identification software at least once a month.
8. Whenever feasible and cost-effective, system developers must rely on system services for security functionality rather than incorporating such functionality into applications. Examples of system services include operating systems, network operating systems, database management systems, access control packages, front-end processors, firewalls, gateways, and routers.
9. All information systems designs will include an IT security plan. This plan will be reviewed for compliance with security policies and standards and to ensure that risks associated with the system are eliminated or reduced to an acceptable level. The Center/Office Information Systems Security Officer (ISSO) must approve the plan and a Designated Approving Authority (DAA) must approve the system prior to initial operation.

b. **Controls And Business Considerations.**

1. Information systems security risk assessments for critical information systems and mission critical applications must be performed at the time of system development (prior to initial operation) and at least once every two years thereafter. All major enhancements, upgrades, conversions, and related changes

associated with these systems or applications must be preceded by a risk assessment and a revised security plan.

2. To minimize costs down and facilitate systems development, FDA must purchase commercially-available information security solutions rather than build the solutions in-house. Exceptions to this policy must only be made when the cost-effectiveness of an in-house solution has been clearly analyzed, documented, and approved by the Center/Office Information System Security Officer.
3. If all essential functional requirements can otherwise be met, an information systems security product which has been evaluated by the US Government or a recognized security authority is preferred and must be used rather than a product which has not been evaluated.
4. FDA information systems must employ recognized information security standards. No exceptions are permitted unless it can be demonstrated that the costs of using a standard exceed the benefits, or that use of a standard will clearly impede FDA's business activities.
5. FDA acknowledges the complexity of legal requirements found in the global networking environment created by the Internet. FDA's information security policies were drafted to meet, and in some instances exceed the protections found in existing laws and regulations. If any FDA information security policy is believed to be in conflict with existing laws or regulations, this observation must be promptly reported to the Center/Office Information System Security Officer.
6. Exceptions to information security policies will be permitted in rare instances where a risk analysis examining the implications of being out of compliance has been performed, where a standard risk acceptance form has been prepared by the responsible manager, and where this form has been approved by the Center/Office Information System Security Officer (ISSO).
7. At the very least, all FDA information systems must include standard controls found in other government organizations facing similar circumstances. Beyond this, the unique risks faced by FDA must be addressed with custom solutions. For every significant information systems security risk, management must make a specific decision about the degree to which FDA will accept the risk or adjust controls to reduce expected losses.
8. Management must allocate sufficient resources and staff attention to adequately address information systems security.

4. **RESPONSIBILITIES.**

a. **Chief Information Officer (CIO).**

The CIO has the overall responsibility for management of the Agency IT security program, including security control selection. The CIO is responsible for ensuring that suitable and appropriate controls are selected for all systems in place or in development and that control selection policies and standards are developed, implemented, and maintained.

b. **FDA Information Systems Security Officer.**

The FDA ISSO, appointed by the CIO, serves as the Agency focal point to direct and oversee the IT security program within the Agency, including security control selection. Responsibilities include the creation of control selection security policies, procedures, standards, and guidance, and the provision of advice and assistance to Agency managers and other organizational personnel concerning control selection issues. With the advice of the Center/Office directors, the ISSO will also advise the Center/Office Directors regarding the selection and appointment of Designated Approving Authorities (DAAs).

c. **Center/Office Directors.**

Directors of the major organizational components have the overall responsibility for monitoring compliance with FDA security policies for their Center/Office, including those governing control selection. Center/Office Directors may delegate the authority for ensuring proper security control selection as appropriate to their organization. Center/Office Directors will appoint a DAA for their Center/Office.

d. **Designated Approving Authority (DAA).**

The DAA for each Center/Office shall be a management official, who, via his signature on an IT security plan, formally assumes responsibility for operation of a specific system at an acceptable level of risk.

e. **Other Major Participants.**

1. Senior Information Resources Management (IRM) Officials

   Designated senior IRM officials serve as the central focus for all aspects of the security program within a Center/Office. IRM officials are responsible for advising the Center/Office Director, the DAA, and others involved on all aspects of security control selection and implementation.

2. Center/Office Information Systems Security Officers (ISSOs)

Center/Office ISSOs serve as the focal point to direct and oversee access security control selection activities within the Center/Office. Responsibilities include providing technical guidance and support to Center/Office staff regarding the conduct of risk assessments, security system reviews, and control selection and implementation. They will also conduct periodic reviews to ensure compliance with applicable policies, and will report on the effectiveness of these policies to appropriate Center/Office management. Center/Office ISSOs will investigate or cause to be investigated known or suspected security control policy violation.

3. System-Specific ISSOs or System Managers

   System-specific ISSOs (i.e., system managers) will ensure that security controls selections are suitable and appropriate to the systems in question. They will also ensure that control selections are fully and properly implemented.

4. System Development Project Managers

   The individual tasked as project manager (PM) for a specific system development effort must be aware of and comply with security control selection policies and procedures relating to information systems. The PM must ensure that control selection and implementation is considered at all stages in the system life cycle. The PM will comply with instructions by the DAA to modify the system in order to comply with applicable security requirements.

5. System Developers (Programmers and Engineers)

   System developers will be aware of and will comply with FDA system life cycle policies, standards, and guidelines, especially as they relate to security control selection.

6. Employees

   Employees who use automated information systems are responsible for complying with all security requirements pertaining to data they use and are accountable for all activity performed under their User ID/password. Employees will report any problem relating to security controls to their supervisor or to the system-specific ISSO or system manager. Employees are required to act ethically, take initiative, and accept responsibility for safeguarding information resources under their control, whether that control is official or de facto.

5. **DEFINITIONS.**

Accreditation. Accreditation is the official management authorization to operate or use a system. It is made on the basis of a certification by designated technical personnel that the system meets pre-specified technical requirements for achieving adequate information protection and systems security.

Automated Information System (AIS). An AIS is an electronically based system configured for the collection, processing, transmission and/or dissemination of information.

Certification. Certification is conducted in support of the accreditation process. It is a technical evaluation that establishes the extent to which a computer system or network design and implementation meet a pre-specified set of security requirements.

Computer Security Incident. A computer security incident is an adverse event affecting a computer system and/or network and its data. The definition of an incident also includes the threat of an adverse event.

Contingency Plan. A contingency plan is developed for an IT system or installation to ensure continuity of support should events occur that disrupt normal operations. Specifically, the plan should provide for continuity of applications critical to essential mission(s) of the users and provide for recovery after a disaster.

Control. A control is a feature or function which limits access to or use of an information resource, which tracks the use of a resource, or which imposes and enforces a requirement to take certain security-related actions.

Designated Approving Authority (DAA). The Designated Approving Authority is a management official, who, via signature on an IT security plan, formally assumes responsibility for operation of a specific system at an acceptable level of risk.

General Support System. A general support system is an interconnected set of information resources under the same direct management control that shares common functionality. The purpose of a general support system is to provide processing or communications support. It typically includes hardware, software, information, data, applications, communications, facilities, and people. A system can be, for example, a local area network, a communications network, or a data processing center.

Least Privilege. Least privilege is the standard practice of restricting user access (to data files, processing capability, or peripherals) or type of access (read, write, execute, delete) to the minimum necessary to perform an authorized job function.

Major Applications. Major applications are systems that require special management attention due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the system (e.g., financial systems).

Risk Management. Risk management is the process of assessing risk and taking steps to reduce and maintain risk at an acceptable level.

Sanitized information. Sanitized information is mission critical information that no longer contains specific details that might be valuable, sensitive, or non-public. It is kept separate from mission critical information.

Separation of Duties. Separation of duties refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process. For example, in financial systems, one person initiates a request for a payment and another authorizes that same payment.

Security Safeguards. Security safeguards are the protective measures and controls that are prescribed to meet the security requirements specified for a system. These safeguards may include, but are not limited to, hardware and software security features; operational procedures; accountability procedures; access and distribution controls; management constraints; personnel security; and physical structures.

Sensitive Data. Sensitive data is any information whose loss, misuse, unauthorized access to, or modification of, could adversely affect the national interest or the conduct of Federal programs, or privacy to which individuals are entitled, but which has not been specifically authorized to be kept secret in the interest of national defense or foreign policy, etc. For purposes of this policy, this relates to industry (e.g., proprietary, patented), copyrighted or business data, as well as data that is simply inappropriate for general viewing.

Security Plan. A security plan is a document that contains detailed technical information about a system, its requirements, and the controls implemented to provide protection against unauthorized disclosure, modification, or destruction of data, and/or denial of service.

Threat. A threat is any circumstance with the potential to cause a harmful event to occur. The four basic threats to an IT system are unauthorized disclosure, destruction, modification, and service denial.

User. Any person using an FDA information system, whether an FDA employee, an employee of another federal, state, or local government agency, a contractor working on-site, or other individual with a valid need to use an FDA system. The user is usually also the system owner.

Vulnerability. Vulnerability is any system flaw or weakness which may be exploited by a specific threat, attack, or harmful event and cause an undesired event or consequence to occur.

6. **EFFECTIVE DATE.** June 1, 2000.

GUIDE - 3250.27
GENERAL MANAGEMENT AND ADMINISTRATION

FOOD AND DRUG ADMINISTRATION

INFORMATION RESOURCES MANAGEMENT - INFORMATION TECHNOLOGY SECURITY

ADMINISTRATIVE SECURITY - OUTSOURCING AND THIRD-PARTY CONTRACTS

1. **PURPOSE.** The purpose of this document is to outline overall Agency-wide policies regarding the security aspects of outsourcing and third-party contracts. The policy describes the general requirements for outsourcing and third-party contracts needed to meet the basic goals of protecting Food and Drug Administration (FDA) automated information; assuring operational continuity, integrity, availability, and confidentiality of automated information; reducing Information Technology (IT) security risk; and, complying with applicable security-related rules and regulations. The policy also outlines the responsibilities of key personnel in support of such requirements.

2. **BACKGROUND.** From time to time, the FDA may perform portions of its information systems operations and management operations through outsourcing and/or third-party contracts. This policy imposes certain requirements on those contracts specifically to meet FDA security needs. In accordance with Federal mandates (see 3. References), the Agency is required to provide "adequate security" to manage potential risk to its automated information. Adequate security includes the imposition of requirements which ensure that third-party or outsource contractors comply with FDA standards regarding the handling of sensitive data. This allows the FDA to compel outsourcers to control the risk and magnitude of the harm that security incidents can cause and which could adversely affect the ability of the FDA to accomplish its mission.

3. **REFERENCES.**

   Computer Security Act of 1987

   Computer Fraud and Abuse Act of 1986

   Clinger-Cohen Act of 1996

   Paperwork Reduction Act of 1995

Federal Managers Financial Integrity Act

Government Information Security Reform Act (GISRA)

Office of Management and Budget (OMB) Circular A-130, Appendix III, "Management of Federal Information Resources," Revised 2/96

DHHS Automated Information Systems Security Program Handbook (Release 2.0), 5/94

Personnel Security/Suitability Program, DHHS Personnel Manual, 1/98

National Institute of Standards and Technology (NIST) Special Publications:

NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, 10/95

NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, 9/96

NIST Special Publication: Information Technology Security Training Requirements: A Role and Performance-Based Model, 1998

NIST User Guide for Developing and Evaluating Security Plans for Unclassified Federal Automated Information Systems (Draft version 6.03)

FDA security plan formats

FDA contingency plan formats

FDA model security (hypothetical) plans

4. **POLICY.** It is the policy of FDA to include definitive provisions for handling of FDA data in any outsourcing or third-party contract. It is further FDA policy that all contracts will provide for termination at no expense to the government in the event of security violations. Each Center/Office must assure that its outsourcing or third-party contracts meet FDA security goals by compliance with the following requirements:
    a. **Third-party Involvement.**
        1. If procurement of third-party software is being considered, management must obtain a written integrity statement from the involved vendor, or conduct testing/monitoring on the software to verify its integrity. This statement must provide assurances that the software in question does not contain hidden mechanisms that could be used to compromise the software's security and will not

require the modification or abandonment of controls found in the operating system under which it runs.

2. All third-party software written for the FDA or any of its subordinate offices, organizations, or divisions, becomes property of the FDA and of the United States Government.

b. **Outsourcing And Third-party Contracts.**

1. All agreements dealing with the handling of FDA information by third parties must include a special clause. This clause must allow FDA to audit the controls used for these information handling activities, and to specify the ways in which FDA information will be protected.
2. Before any third-party users are permitted to reach FDA systems via real-time computer connections, specific written approval of the Center/Office Information System Security officer is required. Requests for approvals must specify the security related responsibilities of FDA, the security related responsibilities of the common carrier (if used), and the security related responsibilities of all other involved third parties. These responsibility statements must also address the liability exposures of the involved parties. An exception to this policy is access to public sources of FDA information such as web sites and Internet pages.
3. All information-systems-related outsourcing contracts must be reviewed and approved by the originating Center/Office Information System Security Officer. It is this officer's responsibility to make sure that these contracts sufficiently define information security responsibilities, as well as how to respond to a variety of potential security problems. It is also this officer's responsibility to make sure that all such contracts allow FDA to terminate the contract for cause if it can be shown that the outsourcing firm does not abide by the information security terms of the contract. Such terminations for cause shall be at no expense to the government.

5. **RESPONSIBILITIES.**

a. **Chief Information Officer (CIO).**

The CIO has the overall responsibility for management of the Agency IT security program, including the security aspects of outsourcing and third-party contracts. The CIO is responsible for ensuring that suitable and appropriate provisions are included in contracts as necessary to ensure the protection of FDA sensitive data and that appropriate remedies are provisioned in the event of a security violation.

b. **FDA Information Systems Security Officer.**

The FDA ISSO, appointed by the CIO, serves as the Agency focal point to direct and oversee the IT security program within the Agency, including

the security of outsourcing and third-party contracts. Responsibilities include reviewing all outsourcing and third-party contracts to ensure that appropriate language is used, and giving advice and assistance to Agency managers and other organizational personnel concerning such contracts and provisions.

c. **Center/Office Directors.**

Directors of the major organizational components have the overall responsibility for monitoring compliance with FDA security policies for their Center/Office, including those that govern outsourcing and third-party contracts. Center/Office Directors may delegate the authority for ensuring that proper outsourcing and third-party contracts requirements are met as appropriate to their organization.

d. **Contracting Officers.**

Contracting officers and specialists will ensure that appropriate definitive provisions for handling of FDA data are incorporated into Statements of Work (SOW), performance standards, and other applicable portions of outsourcing and third-party contracts. Contracting officers will provide for penalties up to and including termination at no expense to the government in the event of security violations or other failures to comply with FDA security requirements commensurate with the criticality of the system involved.

e. **Other Major Participants.**

1. Senior Information Resources Management (IRM) Officials

   Designated senior IRM officials serve as the central focus for all aspects of the security program within a Center/Office, including areas relating to outsourcing and third-party contracts. IRM officials are responsible for advising the Center/Office Director and others involved on all security aspects of outsourcing and third-party contracts.

2. Center/Office Information Systems Security Officers (ISSOs)

   Center/Office ISSOs serve as the focal point to direct and oversee the security aspects of outsourced operations and third-party contract activities within the Center/Office. Responsibilities include providing technical guidance and support to Center/Office staff on issues relating to the security aspects of outsourcing and third-party contracts. They will also conduct periodic reviews to ensure compliance with applicable policies and will report on the effectiveness of these policies to appropriate Center/Office

management. Center/Office ISSOs will investigate or cause to be investigated known or suspected cases of unauthorized actions, improper procedures, and any related policy violation.

3. System-Specific ISSOs or System Managers

   System-specific ISSOs (i.e., system managers) will ensure that suitable and appropriate provisions relating to system security are written into all third-party and outsourcing contracts relative to their systems. They will also ensure that such provisions are fully and properly implemented as necessary.

4. System Development Project Managers

   The individual tasked as project manager (PM) for a specific system development effort must be aware of and comply with third-party and outsourcing contract policies and procedures. They will monitor the performance of all contracts within the scope of their projects to ensure full compliance or to initiate remedial/punitive action.

6. **DEFINITIONS.**

Accreditation. Accreditation is the official management authorization to operate or use a system. It is made on the basis of a certification by designated technical personnel that the system meets pre-specified technical requirements for achieving adequate information protection and systems security.

Automated Information System (AIS). An AIS is an electronically based system configured for the collection, processing, transmission and/or dissemination of information.

Certification. Certification is conducted in support of the accreditation process. It is a technical evaluation that establishes the extent to which a computer system or network design and implementation meet a pre-specified set of security requirements.

Computer Security Incident. A computer security incident is an adverse event affecting a computer system and/or network and its data. The definition of an incident also includes the threat of an adverse event.

Contingency Plan. A contingency plan is developed for an IT system or installation to ensure continuity of support should events occur that disrupt normal operations. Specifically, the plan should provide for continuity of applications critical to essential mission(s) of the users and provide for recovery after a disaster.

Control. A control is a feature or function which limits access to or use of an information resource, which tracks the use of a resource, or which imposes and enforces a requirement to take certain security-related actions.

Designated Approving Authority (DAA). The designated approving authority is a management official, who, via signature on an IT security plan, formally assumes responsibility for operation of a specific system at an acceptable level of risk.

General Support System. A general support system is an interconnected set of information resources under the same direct management control that shares common functionality. The purpose of a general support system is to provide processing or communications support. It typically includes hardware, software, information, data, applications, communications, facilities, and people. A system can be, for example, a local area network, a communications network, or a data processing center.

Least Privilege. Least privilege is the standard practice of restricting user access (to data files, processing capability, or peripherals) or type of access (read, write, execute, delete) to the minimum necessary to perform an authorized job function.

Major Applications. Major applications are systems that require special management attention due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the system (e.g., financial systems).

Outsourcing. Outsourcing is obtaining a major business process or operation by contract from an outside source. Outsource operations usually include functions for which the organization cannot reach economy of scale but which the outsource provider can through aggregation with other clients.

Risk Management. Risk management is the process of assessing risk and taking steps to reduce and maintain risk at an acceptable level.

Sanitized information. Sanitized information is mission critical information that no longer contains specific details that might be valuable, sensitive, or non-public. It is kept separate from mission critical information.

Separation of Duties. Separation of duties refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process. For example, in financial systems, one person initiates a request for a payment and another authorizes that same payment.

Security Safeguards. Security safeguards are the protective measures and controls that are prescribed to meet the security requirements specified for a system. These safeguards may include, but are not limited to, hardware and

software security features; operational procedures; accountability procedures; access and distribution controls; management constraints; personnel security; and physical structures.

Sensitive Data. Sensitive data is any information whose loss, misuse, unauthorized access to, or modification of, could adversely affect the national interest or the conduct of Federal programs, or privacy to which individuals are entitled, but which has not been specifically authorized to be kept secret in the interest of national defense or foreign policy, etc. For purposes of this policy, this relates to industry (e.g., proprietary, patented), copyrighted or business data, as well as data that is simply inappropriate for general viewing.

Security Plan. A security plan is a document that contains detailed technical information about a system, its requirements, and the controls implemented to provide protection against unauthorized disclosure, modification, or destruction of data, and/or denial of service.

Third-Party. A third-party is one with no ties to either party in a contract who may be used as an arbitrator, independent verifier, or other "honest broker".

Threat. A threat is any circumstance with the potential to cause a harmful event to occur. The four basic threats to an IT system are unauthorized disclosure, destruction, modification, and service denial.

User. Any person using an FDA information system, whether an FDA employee, an employee of another federal, state, or local government agency, a contractor working on-site, or other individual with a valid need to use an FDA system. The user is usually also the system owner.

Vulnerability. Vulnerability is any system flaw or weakness which may be exploited by a specific threat, attack, or harmful event and cause an undesired event or consequence to occur.

7. **EFFECTIVE DATE.** June 1, 2001.